The Degraded Gaussian Diamond-Wiretap Channel

Si-Hyeon Lee and Ashish Khisti
Electrical and Computer Engineering, University of Toronto, Toronto, Canada
Email: sihyeon.lee@utoronto.ca, akhisti@comm.utoronto.ca

Abstract

In this paper, we present nontrivial upper and lower bounds on the secrecy capacity of the degraded Gaussian diamond-wiretap channel and identify several ranges of channel parameters where these bounds coincide with useful intuitions. Furthermore, we investigate the effect of the presence of an eavesdropper on the capacity. We consider the following two scenarios regarding the availability of randomness: 1) a common randomness is available at the source and the two relays and 2) a randomness is available only at the source and there is no available randomness at the relays. We obtain the upper bound by taking into account the correlation between the two relay signals and the availability of randomness at each encoder. For the lower bound, we propose two types of coding schemes: 1) a decode-and-forward scheme where the relays cooperatively transmit the message and the fictitious message and 2) a partial DF scheme incorporated with multicoding in which each relay sends an independent partial message and the whole or partial fictitious message using dependent codewords.

Index Terms

Wiretap channel, diamond channel, diamond-wiretap channel, multicoding

I. Introduction

The diamond channel introduced by Schein [1] consists of a broadcast channel (BC) from a source to two relays and a multiple access channel (MAC) from the two relays to a destination. The capacity of the diamond channel is not known in general. To simplify the problem, let us consider a diamond channel having BC with two orthogonal links and Gaussian MAC. In this setup, there is a tension between

This work was supported by QNRF, a member of Qatar Foundation, under NPRP project 5-401-2-161.

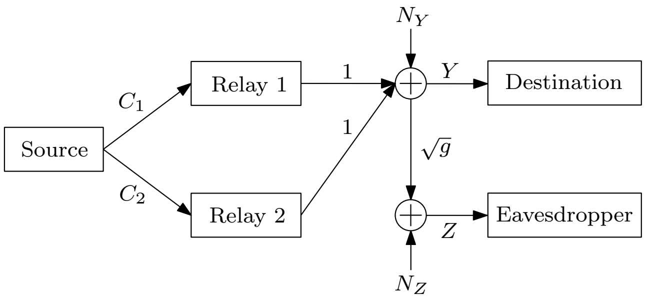


Fig. 1. Physically degraded diamond-wiretap channel

increasing the amount of information sent over the BC and increasing the coherent combining gain for the MAC. Two coding schemes corresponding to the extremes would be partial decode-and-forward, where independent partial messages are sent to the relays, and decode-and-forward (DF), where the whole message is sent to each of the relays. By incorporating multicoding at the source, [2], [3] proposed a coding scheme in which the relays send independent partial messages using dependent codewords and showed that this coding scheme strictly outperforms the DF and partial DF in some regime. Furthermore, [3] showed an upper bound by taking into account the correlation between the two relay signals, which is strictly tighter than the cutset bound. This upper bound was shown to coincide with the lower bound of [2], [3] for some channel parameters.

In this paper, we consider the degraded Gaussian diamond-wiretap channel presented in Fig. 1 and present lower and upper bounds on the secrecy capacity by exploiting the correlation between the two relay signals. We identify several ranges of channel parameters where these bounds coincide with useful intuitions and investigate the effect of the presence of an eavesdropper on the capacity. We note that this model is a natural first step to studying diamond-wiretap channel because the sum secrecy capacity of the multiple access-wiretap channel has been characterized only for the degraded Gaussian case [4]. A practical situation corresponding to this model is the side channel attack [5] where the eavesdropper attacks by probing the physical signals such as timing information and power consumption leaked from the legitimate destination. In the presence of an eavesdropper, the technique of utilizing randomness is widely used to confuse the eavesdropper. We consider the following two scenarios regarding the availability of randomness: 1) a common randomness of rate R' is available at the source and the two relays and 2) a randomness of rate R' is available only at the source and there is no available randomness at the relays. See [6], [7] for the related works assuming restricted randomness at encoders.

For the upper bound, we generalize the upper bound on the capacity of the diamond channel [3] and the upper bound on the sum secrecy capacity of the multiple access-wiretap channel [4]. For the lower bound, we propose two types of coding schemes: 1) a decode-and-forward (DF) scheme where the relays cooperatively transmit the message and the fictitious message and 2) a partial DF scheme incorporated with multicoding in which each relay sends an independent partial message and the whole or partial fictitious message using dependent codewords. If there is no secrecy constraint, our partial DF scheme incorporated with multicoding falls back to that in [2], [3]. Interestingly, in the presence of the eavesdropper, the availability of randomness at the encoders is shown to affect the optimal selection of correlation coefficient between the two relay signals in our proposed schemes.

The remaining this paper is organized as follows. In Section II, we formally present the model of the degraded Gaussian diamond-wiretap channel. Our main results on the secrecy capacity are given in Section III. In Section IV, we derive our upper and lower bounds on the secrecy capacity. We conclude this paper in Section V.

II. Model

Consider the degraded Gaussian diamond-wiretap channel in Fig. 1 that consists of a source, two relays, a legitimate destination, and an eavesdropper. The source is connected to two relays through orthogonal links of capacities C_1 and C_2 and there is no direct link from the source to the legitimate destination or eavesdropper. The channel outputs Y and Z at the legitimate destination and the eavesdropper, respectively, are given as $Y = X_1 + X_2 + N_Y$ and $Z = \sqrt{g}Y + N_Z$, where $g \in [0, 1)$, X_1 and X_2 are the channel inputs from relay 1 and relay 2, respectively, N_Y is the Gaussian noise with zero mean and unit variance at the legitimate destination, and N_Z is the Gaussian noise with zero mean and variance of $1 - g$ at the eavesdropper. N_Y and N_Z are assumed to be independent. The transmit power constraint at relay $k = 1, 2$ is given as $\frac{1}{n}\sum_{i=1}^{n} X_{k,i}^2 \leq P_k$, where n denotes the number of channel uses. Note that the channel output at the eavesdropper is a physically degraded version of the channel output at the legitimate destination.

We consider the following two scenarios regarding the availability of randomness. In the first scenario, a common fictitious message M of rate R', i.e., $M \sim$ Unif$[1 : 2^{nR'}]$[1] is available at the source and the two relays. In this case, a $(2^{nR}, n)$ secrecy code consists of a message $W \sim$ Unif$[1 : 2^{nR}]$, an encoding function at the source that maps $(W, M) \in [1 : 2^{nR}] \times [1 : 2^{nR'}]$ to $(J_1, J_2) \in [1 : 2^{nC_1}] \times [1 : 2^{nC_2}]$, an encoding function at relay $k = 1, 2$ that maps $(J_k, M) \in [1 : 2^{nC_k}] \times [1 : 2^{nR'}]$ to $X_k^n \in \mathcal{X}_k^n$,

[1] $[i : j]$ for two integers i and j denotes the set $\{i, i + 1, \ldots, j\}$.

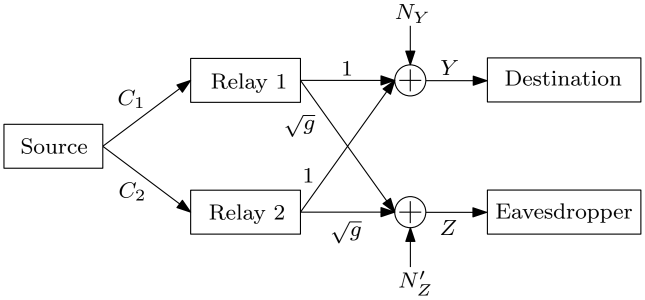


Fig. 2. Stochastically degraded diamond-wiretap channel

and a decoding function at the legitimate destination that maps $Y^n \in \mathcal{Y}^n$ to $\hat{W} \in [1:2^{nR}]$. In the second scenario, a fictitious message M of rate R' is available only at the source and the encoding at the two relays is restricted to be deterministic. In this case, the encoding function at relay $k = 1, 2$ maps $J_k \in [1:2^{nC_k}]$ to $X_k^n \in \mathcal{X}_k^n$.

For both scenarios, the probability of error is given as $P_e^{(n)} = P(\hat{W} \neq W)$. A secrecy rate of R is said to be achievable if there exists a sequence of $(2^{nR}, n)$ codes such that $\lim_{n\to\infty} P_e^{(n)} = 0$ and $\lim_{n\to\infty} \frac{1}{n} I(W; Z^n) = 0$. The secrecy capacity is the supremum of all achievable secrecy rates. Let $C_S^{(1)}$ and $C_S^{(2)}$ denote the secrecy capacity for the first scenario and for the second scenario, respectively.

Remark 1: Because the legitimate destination and the eavesdropper do not cooperate, the secrecy capacity in Fig. 1 is the same as that of stochastically degraded case in Fig. 2, in which Z is given as $Z = \sqrt{g}X_1 + \sqrt{g}X_2 + N'_Z$, where N'_Z has zero mean and unit variance and is independent of N_Y.

III. Main Results

In this section, we present main results of this paper on the secrecy capacity of the degraded Gaussian diamond-wiretap channel described in Section II. For the brevity of presentation, let us define the following functions:

$$f_1(\rho) = C_1 + \frac{1}{2}\log(1 + (1-\rho^2)P_2) \tag{1a}$$

$$f_2(\rho) = C_2 + \frac{1}{2}\log(1 + (1-\rho^2)P_1) \tag{1b}$$

$$f_3(\rho) = C_1 + C_2 - \frac{1}{2}\log(\frac{1}{1-\rho^2}) \tag{1c}$$

$$f_4(\rho) = \frac{1}{2}\log(1 + P_1 + P_2 + 2\rho\sqrt{P_1P_2}) \tag{1d}$$

$$f_5(\rho) = \frac{1}{2}\log(1 + g(P_1 + P_2 + 2\rho\sqrt{P_1P_2})) \tag{1e}$$

$$f_6(\rho) = \frac{1}{2}\log\left(\frac{1+g(P_1+P_2+2\rho\sqrt{P_1P_2})}{1+g(1-\rho^2)P_2}\right) \tag{1f}$$

$$f_7(\rho) = \frac{1}{2}\log\left(\frac{1+g(P_1+P_2+2\rho\sqrt{P_1P_2})}{1+g(1-\rho^2)P_1}\right), \tag{1g}$$

where the domain of f_1, f_2, f_3, f_6, and f_7 is $[-1,1]$ and that of f_4 and f_5 is $[-\bar{\rho}, 1]$ for $\bar{\rho} = \frac{P_1+P_2}{2\sqrt{P_1P_2}}$.[2]

The following two theorems give upper and lower bounds on $C_S^{(1)}$, respectively, whose proofs are in Section IV.

Theorem 1: For $R' \geq 0$, $C_S^{(1)}$ is upper-bounded by

$$\min(\max(S_1, S_2), \max(S_3, S_4)),$$

where

$$S_1 = \max_{0\leq\rho\leq\rho^*} \min(f_1(\rho), f_2(\rho), f_3(\rho), f_4(\rho))$$

$$S_2 = \max_{\rho^*<\rho\leq 1} \min(f_1(\rho), f_2(\rho), f_3(0), f_4(\rho))$$

$$S_3 = \max_{0\leq\rho\leq\rho^*} \min(f_1(\rho), f_2(\rho), f_3(0), \frac{f_3(\rho)+f_4(\rho)}{2}, f_4(\rho)-f_5(\rho))$$

$$S_4 = \max_{\rho^*<\rho\leq 1} \min(f_1(\rho), f_2(\rho), f_3(0), f_4(\rho)-f_5(\rho))$$

for $\rho^* = \sqrt{1+\frac{1}{4P_1P_2}} - \frac{1}{2\sqrt{P_1P_2}}$. We note that the functions f_k's for $k \in [1:5]$ are defined in (1).

Theorem 2: For $\rho \in [-1,1]$ and $R' \geq f_5(\rho)$, $C_S^{(1)}$ is lower-bounded by

$$\max(R_{\mathrm{DF}}^{(1)}(\rho), R_{\mathrm{PDF-M}}^{(1)}(\rho)),$$

where

$$R_{\mathrm{DF}}^{(1)}(\rho) = \min(C_1, C_2, f_4(\rho) - f_5(\rho))$$

$$R_{\mathrm{PDF-M}}^{(1)}(\rho) = \min(f_1(\rho), f_2(\rho), f_3(\rho), f_4(\rho) - f_5(\rho)).$$

We note that the functions f_k's for $k \in [1:5]$ are defined in (1).

In Theorem 1, we note that the upper bound $\max(S_1, S_2)$ is the same as that in [3] that assumes no secrecy constraint. This is natural because the secrecy capacity is upper-bounded by the capacity without secrecy constraint, which is not affected by the common randomness at the encoders. To derive the upper bound $\max(S_3, S_4)$, we generalize the bounding techniques [3] and [4] taking into account the secrecy constraint and the available randomness at the encoders.

[2] By convention, we assume that $f_3(\rho)$ becomes negative infinity when $|\rho| = 1$.

In Theorem 2, $R_{\mathrm{DF}}^{(1)}(\rho)$ is achieved by using a DF scheme where the source sends the message to both relays and the relays cooperatively transmit the message and the common fictitious message over the wiretap channel. On the other hand, $R_{\mathrm{PDF-M}}^{(1)}(\rho)$ is achieved by a partial DF incorporated with multicoding (PDF-M) where each relay sends an independent partial message and the common fictitious message using dependent codewords. The source performs multicoding as follows: the message w is represented as two partial messages (w_1, w_2), a codebook for relay $k = 1, 2$ consisting of independently generated x_k^n sequences is constructed for each w_k and m, and the source finds a jointly typical sequence pair $(x_1^n(w_1, m, l_1), x_2^n(w_2, m, l_2))$ and sends (w_k, l_k) to relay k for $k = 1, 2$. A more detailed explanation for the PDF-M scheme is given in Section IV. Let $R_{\mathrm{PDF}}^{(1)} = R_{\mathrm{PDF-M}}^{(1)}(0)$ denote the partial DF (PDF) rate without multicoding at the source.

To compare our lower and upper bounds, let us consider sufficiently large R' and symmetric channel parameters, i.e., $P_1 = P_2 = P$ and $C_1 = C_2 = C$ for some nonnegative P and C. It can be easily proved that 1) the PDF scheme, which achieves[3] $\min(f_3(0), f_4(0) - f_5(0))$, is optimal for $C \leq \frac{1}{2}(f_4(0) - f_5(0))$, i.e., the BC cut is the bottleneck, and 2) the DF scheme, which achieves $\min(C, f_4(1) - f_5(1))$, is optimal for $C \geq f_4(1) - f_5(1)$, i.e., the MAC cut is the bottleneck. When neither the BC cut nor the MAC cut is the bottleneck, the PDF-M scheme strictly outperforms the PDF and DF schemes for some range of C as shown in Fig. 3. For example, when $P = 1$ and $g = 0.1$, the PDF-M scheme strictly outperforms the PDF and DF schemes for $0.33 < C < 0.89$. Furthermore, Fig. 3 shows that the PDF bound gets close to the upper bound in Theorem 1 as P increases. The following theorem states that the PDF scheme is indeed asymtotically optimal as P_1 or P_2 tends to infinity, whose proof is relegated to the end of this section.

Theorem 3: For the first scenario with $R' \geq f_5(0)$ and $P_1 \to \infty$ or $P_2 \to \infty$,[4] the PDF scheme is asymptotically optimal.

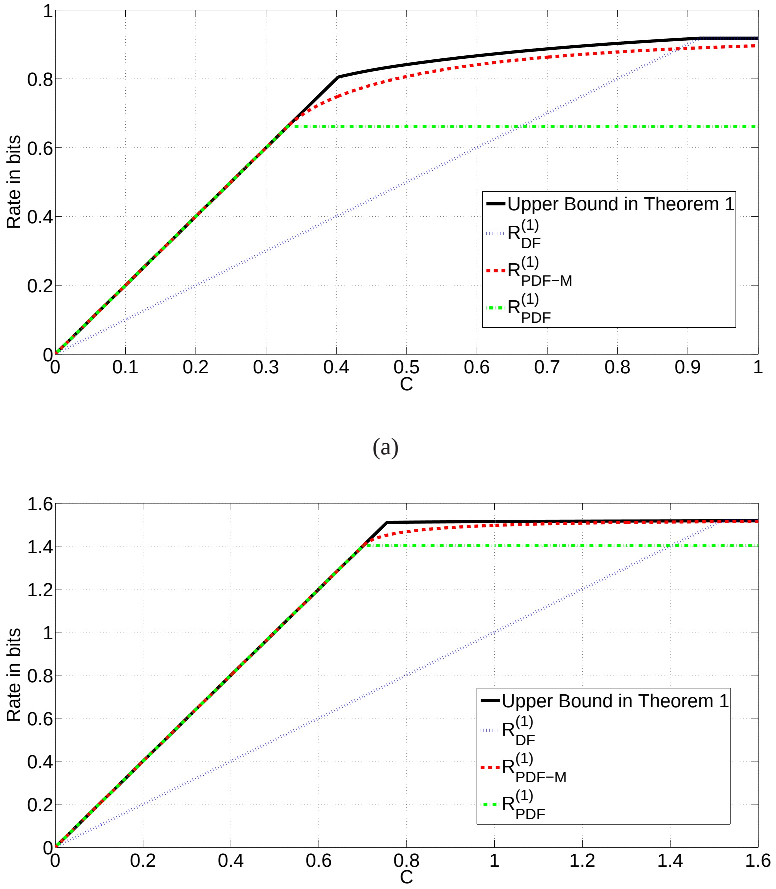
Next, the following two theorems give upper and lower bounds on $C_S^{(2)}$, respectively, whose proofs are in Section IV.

Theorem 4: For $R' \geq 0$, $C_S^{(2)}$ is upper-bounded by

$$\max(T_1, T_2, T_3),$$

[3] For $P_1 = P_2$, $C_1 = C_2 = C$, and $\rho = 0$, $f_1(0)$ and $f_2(0)$ become redundant.

[4] C_1 and C_2 are not necessarily fixed and can be arbitrary functions of P_1 and P_2.



(a)

(b)

Fig. 3. Bounds for the first scenario when (a) $P = 1, g = 0.1$ and (b) $P = 10, g = 0.1$.

where

$$T_1 = \max_{-\bar{\rho}\le\rho<0} \min(f_1(0), f_2(0), f_3(0), f_4(\rho)) - f_5(\rho)$$

$$T_2 = \max_{0\le\rho\le\rho^*} \min(f_1(\rho), f_2(\rho), f_3(\rho), f_4(\rho)) - f_5(\rho)$$

$$T_3 = \max_{\rho^*<\rho\le 1} \min(f_1(\rho), f_2(\rho), f_3(0), f_4(\rho)) - f_5(\rho).$$

We note that the functions f_k's for $k \in [1:5]$ are defined in (1), $\bar{\rho} = \frac{P_1+P_2}{2\sqrt{P_1P_2}}$, and $\rho^* = \sqrt{1 + \frac{1}{4P_1P_2}} - \frac{1}{2\sqrt{P_1P_2}}$.

Theorem 5: For $\rho \in [-1, 1]$ such that $R' \ge f_5(\rho)$, $C_S^{(2)}$ is lower-bounded by

$$\max(R^{(2)}_{\mathrm{DF}}(\rho), R^{(2)}_{\mathrm{PDF-DF-M}}(\rho), R^{(2)}_{\mathrm{PDF-PDF-M}}(\rho)),$$

where

$$R_{\rm DF}^{(2)}(\rho) = \min(C_1, C_2, f_4(\rho)) - f_5(\rho)$$
$$R_{\rm PDF-DF-M}^{(2)}(\rho) = \min(f_1(\rho), f_2(\rho), f_3(\rho) - f_5(\rho), f_4(\rho)) - f_5(\rho)$$
$$R_{\rm PDF-PDF-M}^{(2)}(\rho) = (\min(f_1(\rho), f_2(\rho), f_3(\rho), f_4(\rho)) - f_5(\rho)) \cdot \mathbb{1}_{C_1 > f_6(\rho), C_2 > f_7(\rho)}.$$

We note that the functions f_k's for $k \in [1:7]$ are defined in (1).

Note that in both the upper and lower bounds for the first scenario, the term $f_5(\rho)$, which corresponds to the required rate of randomness to confuse the eavesdropper, appears only with $f_4(\rho)$, which signifies the amount of information sent through the MAC. In contrast, in both the upper and lower bounds for the second scenario, because the fictitious message has to be sent through the BC, $f_5(\rho)$ appears in common for all terms. This affects sufficient ranges of correlation coefficient for the lower bounds for large enough R' as remarked in the following.

Remark 2: For large enough R', sufficient ranges of correlation coefficient ρ for the lower bounds in Theorem 2 and Theorem 5 are different. For the first scenario, note that the DF rate is maximized at $\rho = 1$ and that it is enough to consider nonnegative ρ for the PDF-M scheme. On the other hand, for the second scenario, because the minus term $-f_5(\rho)$ is common for all terms, considering smaller ρ can be beneficial by decreasing $f_5(\rho)$ and we need consider all $-1 \leq \rho \leq 1$.

In the DF scheme for the second scenario, the source sends to both relays the fictitious message as well as the message. Hence, $R_{\rm DF}^{(2)}$ is obtained from $R_{\rm DF}^{(1)}$ by replacing C_1 and C_2 by $C_1 - f_5(\rho)$ and $C_2 - f_5(\rho)$, respectively. For a partial DF scheme incorporated with multicoding for the second scenario, a straightforward extension from that for the first scenario is to let the source send the fictitious message m as well as the partial message w_k and the relay codeword index l_k to relay k for $k = 1, 2$. Since each relay decodes a partial genuine message and a whole fictitious message, we call this scheme as PDF-DF-M scheme. Note that $R_{\rm PDF-DF-M}^{(2)}(\rho)$ is obtained by replacing C_1 and C_2 by $C_1 - f_5(\rho)$ and $C_2 - f_5(\rho)$, respectively, in $R_{\rm PDF-M}^{(1)}$. However, since the same fictitious message is sent to both relays, there exists inefficiency in the use of the BC. To resolve this inefficiency, we let each of relay codebooks be indexed by independent partial fictitious message, i.e., codebook for relay $k = 1, 2$ is constructed for each (w_k, m_k) by representing m as two partial fictitious messages (m_1, m_2). By using this PDF-PDF-M scheme where each relay decodes a partial genuine message and a partial fictitious message, we show that $R_{\rm PDF-PDF-M}^{(2)}(\rho)$ is achievable, which has $f_3(\rho)$ intead of $f_3(\rho) - f_5(\rho)$ in $R_{\rm PDF-DF-M}^{(2)}(\rho)$. We note that having independent fictitious message at each relay reduces the achievable rate region over the MAC, which results in additional contraints $C_1 > f_6(\rho)$ and $C_2 > f_7(\rho)$ in $R_{\rm PDF-PDF-M}^{(2)}(\rho)$.

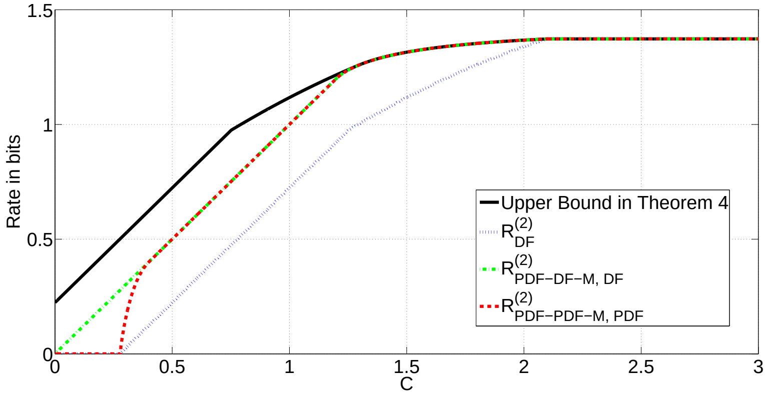
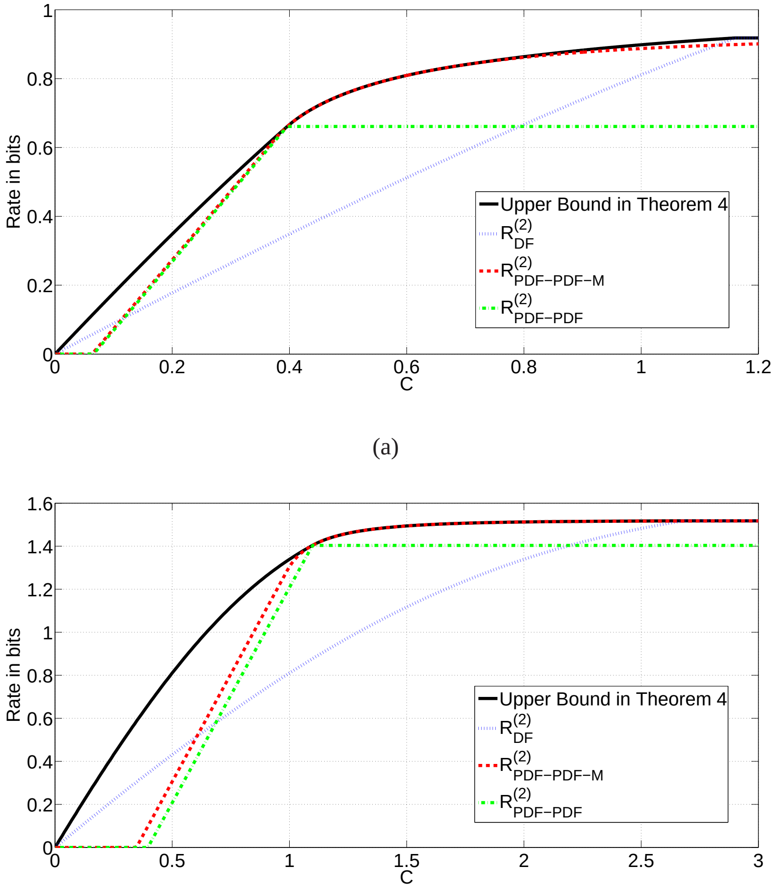


Fig. 4. For sufficiently large R', $g = 0.1$, $C_1 = C$, $C_2 = C + 2$, $P_1 = 10$, and $P_2 = 1$, $R^{(2)}_{\mathrm{PDF-DF-M}}(\rho)$ is strictly higher than $R^{(2)}_{\mathrm{PDF-PDF-M}}(\rho)$ for some range of C.

Nevertheless, as long as $C_1 = C_2$, $R^{(2)}_{\mathrm{PDF-PDF-M}}(\rho)$ is always higher than or equal to $R^{(2)}_{\mathrm{PDF-DF-M}}(\rho)$ because $f_3(\rho) > 2f_5(\rho)$, which should be satisfied if $R^{(2)}_{\mathrm{PDF-DF-M}}(\rho) > 0$, implies $C_1 > f_6(\rho)$ and $C_2 > f_7(\rho)$. If $C_1 \neq C_2$, $R^{(2)}_{\mathrm{PDF-DF-M}}(\rho)$ can be strictly higher than $R^{(2)}_{\mathrm{PDF-PDF-M}}(\rho)$ as illustrated in Fig. 4. Let $R^{(2)}_{\mathrm{PDF-DF}} = R^{(2)}_{\mathrm{PDF-DF-M}}(0)$ and $R^{(2)}_{\mathrm{PDF-PDF}} = R^{(2)}_{\mathrm{PDF-PDF-M}}(0)$ denote the rates of PDF-DF and PDF-PDF schemes (without multicoding).

Similarly as for the first scenario, let us consider sufficiently large R' and symmetric channel parameters. Since $C_1 = C_2$, we only consider the DF, PDF-PDF-M, and PDF-PDF schemes for the lower bounds. It can be easily proved that the DF scheme, which achieves $\max_{\rho\in[-1,1]} \min(C, f_4(\rho)) - f_5(\rho)$, is optimal for $C \geq f_4(1)$, i.e., the MAC cut is the bottleneck. We can see in Fig. 5 that the PDF-PDF rate coincides with the PDF-PDF-M rate at one point. This is because a negative correlation between the two relay signals is helpful for small C due to the reason in Remark 2, i.e., the BC cut is the bottleneck, and positive correlation becomes beneficial as C increases, i.e., the MAC cut becomes bottleneck. Fig. 5 also shows that the PDF-PDF-M rate is zero up to some threshold value of C due to the constraint $C > f_6(\rho)$ in $R^{(2)}_{\mathrm{PDF-PDF-M}}(\rho)$ and the threshold value decreases as P decreases. Indeed, we can prove that the threshold value tends to zero as P tends to zero. Furthermore, Fig. 5 shows that the PDF-PDF-M rate coincides with the upper bound in Theorem 4 for some range of C, e.g., $1.1 < C < 2.18$ when $P = 10$ and $g = 0.1$. The following theorem gives a condition where the PDF-PDF-M rate coincides with the upper bound in Theorems 4, whose proof is relegated to the end of this section.

Theorem 6: For the second scenario with sufficiently large R' and symmetric channel parameters, the



(a)

(b)

Fig. 5. Bounds for the second scenario when (a) $P = 1, g = 0.1$ and (b) $P = 10, g = 0.1$.

PDF-PDF-M rate in Theorem 5 coincide with the upper bound in Theorem 4, and the secrecy capacity is given as $f_3(\rho') - f_5(\rho')$ for

$$\frac{1}{4}\log(1+2P) \le C \le \frac{1}{4}\log(1+2(1+\rho^*)P) + \frac{1}{4}\log(\frac{1}{1-\rho^{*2}}) \tag{2}$$

such that that at least one of $f_1(\rho^*) - f_5(\rho^*) \le f_3(\rho') - f_5(\rho')$ and $f_3(0) - f_5(\rho^*) \le f_3(\rho') - f_5(\rho')$ is satisfied, where $\rho^* = \sqrt{1 + \frac{1}{4P_1P_2}} - \frac{1}{2\sqrt{P_1P_2}}$ and $\rho' \in [0, \rho^*]$ is such that $f_3(\rho') = f_4(\rho')$.[5]

Theorem 6 indicates that the upper and lower bounds in Theorems 4 and 5 coincide for $1.1 < C < 2.18$ when $P = 10$ and $g = 0.1$ and for $1.91 < C < 3.82$ when $P = 100$ and $g = 0.1$.

Remark 3: For $g = 0$, the bounds in Theorems 1-5 fall back to those in [3].

[5] We note that under the condition (2), $\rho' \in [0, \rho^*]$ such that $f_3(\rho') = f_4(\rho')$ exists.

Now, a natural question is how the presence of an eavesdropper affects the capacity. We partially answer this question by comparing our results with the lower and upper bounds in [3] that are derived without secrecy constraint. Note that when there is no secrecy constraint, the availability of randomness at the encoders does not affect the capacity. Hence, the capacity without secrecy constraint is higher than or equal to the secrecy capacity with secrecy constraint both for the first and the second scenarios. We compare the bounds in Fig. 6 for sufficiently large R' and symmetric channel parameters. First, as illustrated in Fig. 6-(a), the upper bound without secrecy constraint and the lower bound for the first scenario coincide up to $C \leq \frac{1}{2}(f_4(0) - f_5(0))$. This indicates that, when there is a sufficient amount of common randomness between the source and the relays, there is no decrease in capacity due to an eavesdropper for some range of C. On the other hand, for the same channel parameters, Fig. 6-(b) shows that the lower bound without secrecy constraint is strictly higher than the upper bound for the second scenario for all range of $C > 0$. This indicates that, when there is no randomness at the relays, the secrecy capacity for the second scenario can be strictly smaller than the capacity without secrecy constraint for all range of C.

Proof of Theorem 3: The bound in Theorem 1 is further upper-bounded as follows:

$$\begin{aligned}\min(\max(S_1, S_2), \max(S_3, S_4)) &\leq \max(S_3, S_4) \\ &\overset{(a)}{\leq} \max_{0\leq\rho\leq1} \min(f_1(0), f_2(0), f_3(0), f_4(\rho) - f_5(\rho)),\end{aligned}$$

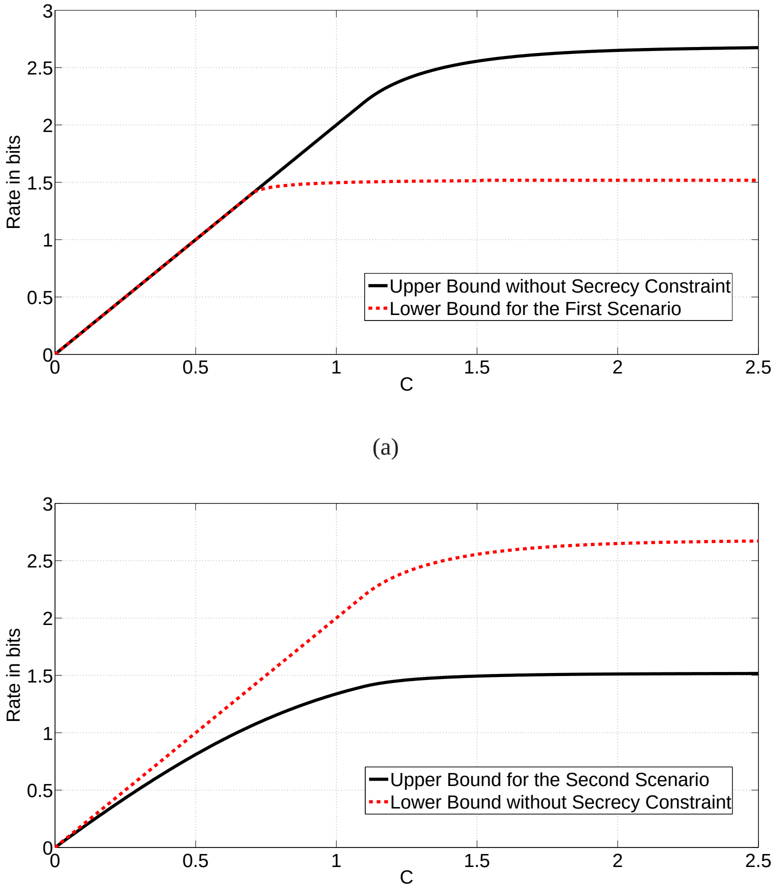
where (a) is because $f_1(\rho)$ and $f_2(\rho)$ are decreasing functions of $\rho \in [0,1]$. Furthermore, for any $\rho \in [0,1]$, we have

$$\begin{aligned}\lim_{P_1\to\infty \text{ or } P_2\to\infty} f_4(\rho) - f_5(\rho) &= \lim_{P_1\to\infty \text{ or } P_2\to\infty} \frac{1}{2}\log\frac{1 + P_1 + P_2 + 2\rho\sqrt{P_1P_2}}{1 + g(P_1 + P_2 + 2\rho\sqrt{P_1P_2})} \\ &= \frac{1}{2}\log\frac{1}{g} \\ &= \lim_{P_1\to\infty \text{ or } P_2\to\infty} f_4(0) - f_5(0).\end{aligned}$$

Hence, the secrecy capacity for the first scenario when $P_1 \to \infty$ or $P_2 \to \infty$ is asymtotically upper-bounded by

$$\lim_{P_1\to\infty \text{ or } P_2\to\infty} \min(f_1(0), f_2(0), f_3(0), f_4(0) - f_5(0)),$$

which is clearly achievable by the PDF scheme. ■



(a)

(b)

Fig. 6. Comparison with the lower and upper bounds without secrecy constraint when $P = 10$ and $g = 0.1$.

Proof of Theorem 6: Let us first show that $\max(T_1, T_2) = f_3(\rho') - f_5(\rho')$. For symmetric channel parameters, T_1 and T_2 can be rewritten as follows:

$$T_1 = \max_{-1 \le \rho < 0} \min(f_3(0), f_4(\rho)) - f_5(\rho)$$

$$T_2 = \max_{0 \le \rho \le \rho^*} \min(f_3(\rho), f_4(\rho)) - f_5(\rho).$$

Let us define functions $f_{35}(\rho)$ and $f_{45}(\rho)$ of $\rho \in [-1, \rho^*]$ as follows:

$$f_{35}(\rho) = \begin{cases} f_3(0) - f_5(\rho) \text{ if } \; -1 \le \rho < 0 \\ f_3(\rho) - f_5(\rho) \text{ otherwise} \end{cases} \quad , \; f_{45}(\rho) = f_4(\rho) - f_5(\rho).$$

Note that we can rewrite the condition in (2) as $f_{35}(0) \ge f_{45}(0)$ and $f_{35}(\rho^*) \le f_{45}(\rho^*)$. Since $f_{35}(\rho)$ and $f_{45}(\rho)$ are monotonically decreasing function and monotonically increasing function of $\rho \in [-1, \rho^*]$, respectively, the condition in (2) implies that there exists $\rho' \in [0, \rho^*]$ such that $f_{35}(\rho') = f_{45}(\rho')$. Hence, we have $\max(T_1, T_2) = \max_{-1\leq\rho\leq\rho^*} \min(f_{35}(\rho), f_{45}(\rho)) = f_{35}(\rho') = f_3(\rho') - f_5(\rho')$.

Now, let us show $\max(f_{35}(\rho'), T_3) = f_{35}(\rho')$. Since both $f_1(\rho) - f_5(\rho)$ and $f_3(0) - f_5(\rho)$ for $\rho \in [\rho^*, 1]$ have the maximum at $\rho = \rho^*$, we have

$$\max(f_{35}(\rho'), T_3) \leq \max(f_{35}(\rho'), \min(f_1(\rho^*) - f_5(\rho^*), f_3(0) - f_5(\rho^*))) = f_{35}(\rho')$$

if $f_1(\rho^*) - f_5(\rho^*) \leq f_3(\rho') - f_5(\rho')$ or $f_3(0) - f_5(\rho^*) \leq f_3(\rho') - f_5(\rho')$. Hence, under the conditions in Theorem 6, the upper bound in Theorem 4 becomes $f_3(\rho') - f_5(\rho')$.

Now, it remains to show $f_3(\rho') - f_5(\rho')$ is achievable. We have

$$\begin{aligned} R^{(2)}_{\mathrm{PDF-PDF-M}}(\rho') &= (f_3(\rho') - f_5(\rho')) \cdot \mathbb{1}_{C > f_6(\rho')} \\ &\overset{(a)}{=} f_3(\rho') - f_5(\rho') \end{aligned}$$

where (a) is because $f_3(\rho') = f_4(\rho')$ and $f_3(\rho') - f_5(\rho') = f_4(\rho') - f_5(\rho') > 0$ imply $C > f_6(\rho')$. This completes the proof. ■

IV. Derivation of Upper and Lower Bounds on the Secrecy Capacity

In this section, we prove the upper and lower bounds on the secrecy capacity presented in Section III.

A. *Proof of Theorem 1*

We note that the upper bound $\max(S_1, S_2)$, which the same as the upper bound in [3] on the capacity without secrecy constraint, is easily obtained by noting that the secrecy capacity is upper-bounded by the capacity without secrecy constraint and that common randomness at the encoders does not affect the capacity when there is no secrecy constraint. Nevertheless, we provide a direct proof for the upper bound $\max(S_1, S_2)$ as well as the upper bound $\max(S_3, S_4)$ since it can be useful for bounding in other related problems.

The proof generalizes those in [3] and [4] taking into account the secrecy constraint and the available randomness at the encoders. For $k \in [1:2]$ and $i \in [1:n]$, let $P_{k,i} = \mathrm{E}(X^2_{k,i})$ and let $\lambda_i = \frac{E(X_{1,i}X_{2,i})}{\sqrt{P_{1,i}P_{2,i}}}$. Let $\lambda_a \in [0,1]$ and $\lambda_b \in [0,1]$ be such that $\lambda_a^2 P_1 = \frac{1}{n}\sum_{i=1}^n \lambda_i^2 P_{1,i}$ and $\lambda_b^2 P_2 = \frac{1}{n}\sum_{i=1}^n \lambda_i^2 P_{2,i}$. We use ϵ_n to denote a function of n such that ϵ_n tends to zero as n tends to infinity.

By applying similar bounding techniques as in [3], we have

$$
\begin{aligned}
nR &= H(W) \\
&\overset{(a)}{\leq} I(W; J_1, Y^n, M) + n\epsilon_n \\
&\overset{(b)}{=} I(W; J_1, Y^n | M) + n\epsilon_n \\
&\leq H(J_1) + I(W; Y^n | J_1, M) + n\epsilon_n \\
&\overset{(c)}{\leq} H(J_1) + I(W; Y^n | J_1, M, X_1^n) + n\epsilon_n \\
&\leq H(J_1) + I(W, X_2^n; Y^n | J_1, M, X_1^n) + n\epsilon_n \\
&\leq nC_1 + I(X_2^n; Y^n | X_1^n) + n\epsilon_n \\
&\leq nC_1 + \sum_{i=1}^{n} I(X_{2,i}; Y_i | X_{1,i}) + n\epsilon_n \\
&\overset{(d)}{\leq} nC_1 + \sum_{i=1}^{n} \log(1 + (1 - \lambda_i^2) P_{2,i}) + n\epsilon_n \\
&\overset{(e)}{\leq} nC_1 + n \log(\frac{1}{n} \sum_{i=1}^{n} (1 + (1 - \lambda_i^2) P_{2,i})) + n\epsilon_n \\
&\overset{(f)}{\leq} nC_1 + n \log(1 + (1 - \lambda_b^2) P_2) + n\epsilon_n
\end{aligned} \tag{3}
$$

for sufficiently large n, where (a) is from the Fano's inequality, (b) is because W and M are independent, (c) is because X_1^n is a function of J_1 and M, (d) is because the Gaussian distribution maximizes the differential entropy given the power constaint, (e) is due to the concavity of the logarithm function, and (f) is from the definition of λ_b. Similarly, we can obtain

$$nR \leq nC_2 + n \log(1 + (1 - \lambda_a^2) P_1) + n\epsilon_n \tag{4}$$

for sufficiently large n.

We also have for sufficiently large n,

$$\begin{aligned} nR &= H(W) \\ &\overset{(a)}{\leq} I(W;Y^n,M)+n\epsilon_n \\ &\overset{(b)}{=} I(W;Y^n|M)+n\epsilon_n \\ &\overset{(c)}{=} I(X_1^n,X_2^n;Y^n|M)+n\epsilon_n \qquad (5) \\ &\leq H(X_1^n,X_2^n|M)+n\epsilon_n \\ &\leq H(X_1^n|M)+H(X_2^n|M)-I(X_1^n;X_2^n|M)+n\epsilon_n \\ &\leq nC_1+nC_2-I(X_1^n;X_2^n|M)+n\epsilon_n, \qquad (6) \end{aligned}$$

where (a) is from the Fano's inequality, (b) is because W and M are independent, and (c) is because X_1^n and X_2^n are functions of M and W and the Markov relationship $W-(M,X_1^n,X_2^n)-Y^n$ holds.

Furthermore, for any random variable U_i generated through a conditional pmf $p(u_i|x_{1,i},x_{2,i},y_i)$, we have

$$\begin{aligned} & I(X_1^n;X_2^n|M) \\ &= I(X_1^n,X_2^n;U^n|M)-I(X_1^n;U^n|X_2^n,M)-I(X_2^n;U^n|X_1^n,M)+I(X_1^n;X_2^n|U^n,M) \\ &\geq I(X_1^n,X_2^n;U^n|M)-I(X_1^n;U^n|X_2^n)-I(X_2^n;U^n|X_1^n). \qquad (7) \end{aligned}$$

By applying the above lower bound to (6), we obtain

$$nR \leq nC_1+nC_2-I(X_1^n,X_2^n;U^n|M)+I(X_1^n;U^n|X_2^n)+I(X_2^n;U^n|X_1^n)+n\epsilon_n. \qquad (8)$$

For sufficiently large n, we have

$$\begin{aligned}
nR &= H(W)\\
&\overset{(a)}{\leq} H(W|Z^n) + n\epsilon_n\\
&\overset{(b)}{\leq} H(W|Z^n) - H(W|Y^n, Z^n) + 2n\epsilon_n\\
&= I(W; Y^n|Z^n) + 2n\epsilon_n\\
&\leq I(X_1^n, X_2^n; Y^n|Z^n) + 2n\epsilon_n\\
&\overset{(c)}{\leq} I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; Z^n) + 2n\epsilon_n \qquad (9)\\
&= h(Y^n) - h(Z^n) + 2n\epsilon_n\\
&\overset{(d)}{\leq} h(Y^n) - \frac{n}{2}\log(g2^{\frac{2}{n}h(Y^n)} + 2\pi e(1-g)) + 2n\epsilon_n, \qquad (10)
\end{aligned}$$

where (a) is from the secrecy constraint, (b) is due to the Fano's inequality, (c) is due to the degradedness of the channel, and (d) is from the entropy power inequality. We note that (10) is a nondecreasing function of $h(Y^n)$. $h(Y^n)$ is further upper-bounded as follows:

$$\begin{aligned}
h(Y^n) &\leq \sum_{i=1}^{n} h(Y_i)\\
&\leq \sum_{i=1}^{n} \frac{1}{2}\log(2\pi e)(1 + P_{1,i} + P_{2,i} + 2\lambda_i\sqrt{P_{1,i}P_{2,i}})\\
&\leq \frac{n}{2}\log(2\pi e)(\frac{1}{n}\sum_{i=1}^{n}(1 + P_{1,i} + P_{2,i} + 2\lambda_i\sqrt{P_{1,i}P_{2,i}}))\\
&\leq \frac{n}{2}\log(2\pi e)(1 + P_1 + P_2 + \frac{2}{n}\sum_{i=1}^{n}\sqrt{\lambda_i^2 P_{1,i}P_{2,i}}).
\end{aligned}$$

From the Cauchy-Schwarz inequality, we have

$$\begin{aligned}
\frac{1}{n}\sum_{i=1}^{n}\sqrt{\lambda_i^2 P_{1,i}P_{2,i}} &\leq \sqrt{(\frac{1}{n}\sum_{i=1}^{n}\lambda_i^2 P_{1,i})(\frac{1}{n}\sum_{i=1}^{n}P_{2,i})}\\
&\leq \sqrt{\lambda_a^2 P_1 P_2}.
\end{aligned}$$

Similarly, we have $\frac{1}{n}\sum_{i=1}^{n}\sqrt{\lambda_i^2 P_{1,i}P_{2,i}} \leq \sqrt{\lambda_b^2 P_1 P_2}$. Hence, we obtain

$$h(Y^n) \leq \frac{n}{2}\log(2\pi e)(1 + P_1 + P_2 + 2\min(\lambda_a, \lambda_b)\sqrt{P_1P_2}). \qquad (11)$$

Now we are ready to prove Theorem 1. Define $\mu \in [0,1]$ and $\nu \in [0,1]$ as follows. First, μ is determined from $h(Y^n|M)$. $\mu = 0$ if

$$\frac{1}{n}h(Y^n|M) \leq \frac{1}{2}\log(2\pi e)(1+P_1+P_2). \tag{12}$$

Otherwise, μ is such that

$$\frac{1}{n}h(Y^n|M) = \frac{1}{2}\log(2\pi e)(1+P_1+P_2+2\mu\sqrt{P_1P_2}). \tag{13}$$

Next, ν is determined from $h(Y^n)$. $\nu = 0$ if

$$\frac{1}{n}h(Y^n) \leq \frac{1}{2}\log(2\pi e)(1+P_1+P_2). \tag{14}$$

Otherwise, ν is such that

$$\frac{1}{n}h(Y^n) = \frac{1}{2}\log(2\pi e)(1+P_1+P_2+2\nu\sqrt{P_1P_2}). \tag{15}$$

Let us first show that

$$R \leq \max(S_1, S_2) + \epsilon_n. \tag{16}$$

If $\mu = 0$, from (3), (4), (6), (5), and (12), we have $R \leq \min(f_1(0), f_2(0), f_3(0), f_4(0)) + \epsilon_n$. Consider $\mu > 0$. From $h(Y^n|M) \leq h(Y^n)$, (13), and (11), we have $\mu \leq \min(\lambda_a, \lambda_b)$. Then, from (3), (4), (6), (5), and (13), we obtain $R \leq \min(f_1(\mu), f_2(\mu), f_3(0), f_4(\mu)) + \epsilon_n$. If μ further satisfies $0 < \mu \leq \rho^*$, we let $U_i = Y_i + V_i$, where V_i is an i.i.d. Gaussian random variable with zero mean and variance of $\gamma = \sqrt{P_1P_2}(\frac{1}{\mu} - \mu) - 1$.[6] Then, the mutual information terms in (8) are bounded as follows:

$$\begin{aligned}
&I(X_1^n, X_2^n; U^n|M) \\
&\geq h(U^n|M) - \frac{n}{2}\log(2\pi e)(1+\gamma) \\
&\overset{(a)}{\geq} \frac{n}{2}\log(2^{\frac{2}{n}h(Y^n|M)} + 2\pi e\gamma) - \frac{n}{2}\log(2\pi e)(1+\gamma) \\
&= \frac{n}{2}\log\frac{1+\gamma+P_1+P_2+2\mu\sqrt{P_1P_2}}{1+\gamma}
\end{aligned} \tag{17}$$

$$I(X_1^n; U^n|X_2^n) \leq \frac{n}{2}\log\frac{1+\gamma+(1-\gamma^2)P_1}{1+\gamma} \tag{18}$$

$$I(X_2^n; U^n|X_1^n) \leq \frac{n}{2}\log\frac{1+\gamma+(1-\gamma^2)P_2}{1+\gamma}, \tag{19}$$

[6] For $0 < \mu \leq \rho^*$, γ is nonnegative.

where (a) is from the conditional entropy power inequality. Substituting the above bounds to (8), we obtain $R \leq f_3(\mu) + \epsilon_n$. Hence, we have $R \leq \min(f_1(\mu), f_2(\mu), f_3(\mu), f_4(\mu)) + \epsilon_n$ for $0 < \mu \leq \rho^*$. This concludes the proof of (16).

Now, let us show

$$R \leq \max(S_3, S_4) + 2\epsilon_n. \tag{20}$$

If $\nu = 0$, from (3), (4), (6), (10), and (14), we have $R \leq \min(f_1(0), f_2(0), f_3(0), f_4(0) - f_5(0)) + 2\epsilon_n$. Consider $\nu > 0$. From (15) and (11), we have $\nu \leq \min(\lambda_a, \lambda_b)$. Then, from (3), (4), (6), (10), and (15), we obtain $R \leq \min(f_1(\mu), f_2(\mu), f_3(0), f_4(\nu) - f_5(\nu)) + 2\epsilon_n$. If ν further satisfies $0 < \nu \leq \rho^*$, we consider the following bound by adding the inequalities (5) and (8):

$$\begin{aligned} 2nR &\leq nC_1 + nC_2 + I(X_1^n, X_2^n; Y^n|M) - I(X_1^n, X_2^n; U^n|M) \\ &\qquad + I(X_1^n; U^n|X_2^n) + I(X_2^n; U^n|X_1^n) + 2n\epsilon_n \\ &\leq nC_1 + nC_2 + I(X_1^n, X_2^n; Y^n|U^n, M) \\ &\qquad + I(X_1^n; U^n|X_2^n) + I(X_2^n; U^n|X_1^n) + 2n\epsilon_n \\ &\leq nC_1 + nC_2 + I(X_1^n, X_2^n; Y^n|U^n) \\ &\qquad + I(X_1^n; U^n|X_2^n) + I(X_2^n; U^n|X_1^n) + 2n\epsilon_n \\ &\overset{(a)}{\leq} nC_1 + nC_2 + I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; U^n) \\ &\qquad + I(X_1^n; U^n|X_2^n) + I(X_2^n; U^n|X_1^n) + 2n\epsilon_n, \end{aligned} \tag{21}$$

where (a) holds when $(X_1^n, X_2^n) - Y^n - U^n$. We let $U_i = Y_i + V_i'$, where V_i' is an i.i.d. Gaussian random variable with zero mean and variance of $\gamma' = \sqrt{P_1P_2}(\frac{1}{\nu} - \nu) - 1$. Then, by substituting (15) and similar bounds as in (17)-(19) to (21), we obtain $R \leq \frac{f_3(\nu)+f_4(\nu)}{2} + \epsilon_n$. Hence, we have $R \leq \min(f_1(\nu), f_2(\nu), f_3(0), \frac{f_3(\nu)+f_4(\nu)}{2},\ f_4(\nu) - f_5(\nu)) + 2\epsilon_n$ for $0 < \nu \leq \rho^*$. This concludes the proof of (20).

B. *Proof of Theorem 2*

Let us first assume that the channel from the relays to the legitimate destination and the eavesdropper is a discrete memoryless channel with a conditional pmf $p(y, z|x_1, x_2)$. Fix $p(x_1, x_2)$ and let

$$R' = I(X_1, X_2; Z) - \delta(\epsilon). \tag{22}$$

Fix $\epsilon > 0$. We use $\delta(\epsilon)$ to denote a function of ϵ such that $\delta(\epsilon)$ tends to zero as ϵ tends to zero.

In the DF scheme, the source sends the message to both relays, which requires $R < \min(C_1, C_2)$. Once the relays share both the message and the fictitious message, we can treat the channel from the relays to the legitimate destination and the eavesdropper as a classical wiretap channel [8], [9] with randomness of rate R' in (22) and hence the secrecy rate of $R < I(X_1, X_2; Y) - I(X_1, X_2; Z)$ is achievable. By combining two inequalities for R, we conclude the following secrecy rate is achievable:

$$\min(C_1, C_2, I(X_1, X_2; Y) - I(X_1, X_2; Z)). \tag{23}$$

The PDF-M scheme is described in the following.

- Codebook generation: We represent the message $w \in [1 : 2^{nR}]$ as the partial message pair $(w_1, w_2) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$ for some $R_1 \geq 0$ and $R_2 \geq 0$ such that

$$R_1 + R_2 = R, \tag{24}$$

  i.e., W_k for $k \in [1 : 2]$ is uniformly distributed over $[1 : 2^{nR_k}]$ and W_1 and W_2 are independent. Consider $\tilde{R}_k \geq 0$ for $k \in [1 : 2]$. For each $k \in [1 : 2]$ and $(w_k, m, l_k) \in [1 : 2^{nR_k}] \times [1 : 2^{nR'}] \times [1 : 2^{n\tilde{R}_k}]$, generate $x_k^n(w_k, m, l_k)$ independently according to $\prod_{i=1}^n p(x_{k,i})$.
- Encoding at the source: For message (w_1, w_2) and fictitious message m, the source finds an (l_1, l_2) such that

$$(x_1^n(w_1, m, l_1), x_2^n(w_2, m, l_2)) \in \mathcal{T}_\epsilon^{(n)}.$$

  For $k \in [1 : 2]$, the source sends (w_k, l_k) to relay k.
- Encoding at relay $k \in [1 : 2]$: Note that fictitious message m is given at relay k. After receiving (w_k, l_k) from the source, relay k sends $x_k^n(w_k, m, l_k)$.
- Decoding at the legitimate destination: The legitimate destination finds $(\hat{w}_1, \hat{w}_2, \hat{m}, \hat{l}_1, \hat{l}_2)$ such that

$$(x_1^n(\hat{w}_1, \hat{m}, \hat{l}_1), x_2^n(\hat{w}_2, \hat{m}, \hat{l}_2), y^n) \in \mathcal{T}_\epsilon^{(n)}.$$

  The legitimate destination declares that $(\hat{w}_1, \hat{w}_2)$ is the message.
- Error analysis: From the mutual covering lemma [10], the encoding error at the source averaged over the codebooks tends to zero as n tends to infinity if

$$\tilde{R}_1 + \tilde{R}_2 > I(X_1; X_2) + \delta(\epsilon). \tag{25}$$

  For $k \in [1 : 2]$, the transmission of (w_k, l_k) from the source to relay k requires

$$R_k + \tilde{R}_k < C_k. \tag{26}$$

From the standard error analysis, the decoding error at the legitimate destination averaged over the codebooks tends to zero as n tends to infinity if

$$R_1 + \tilde{R}_1 < I(X_1; Y|X_2) + I(X_1; X_2) - \delta(\epsilon) \tag{27}$$

$$R_2 + \tilde{R}_2 < I(X_2; Y|X_1) + I(X_1; X_2) - \delta(\epsilon) \tag{28}$$

$$R_1 + R_2 + R' + \tilde{R}_1 + \tilde{R}_2 < I(X_1, X_2; Y) + I(X_1; X_2) - \delta(\epsilon). \tag{29}$$

- Secrecy analysis: We can show $\lim_{n\to\infty} \frac{1}{n} I(W; Z^n|\mathcal{C}) \leq \delta(\epsilon) + \epsilon$ if (22) and the following inequalities are satisfied.

$$\tilde{R}_1 < I(X_1; Z|X_2) + I(X_1; X_2) - \delta(\epsilon) \tag{30}$$

$$\tilde{R}_2 < I(X_2; Z|X_1) + I(X_1; X_2) - \delta(\epsilon) \tag{31}$$

$$R' + \tilde{R}_1 + \tilde{R}_2 < I(X_1, X_2; Z) + I(X_1; X_2) - \delta(\epsilon) \tag{32}$$

See Section IV-E for the detail.

Therefore, there exists a sequence of codes such that $P_e^{(n)}$ tends to zero and $\frac{1}{n} I(W; Z^n) \leq \delta(\epsilon) + \epsilon$ as n tends to infinity if (22), (24)-(32) are satisfied. By performing Fourier-Mozkin elimination to (22), (24)-(32) and by taking $\epsilon \to 0$, the PDF-M rate of

$$\min(C_1 + I(X_2; Y|X_1), C_2 + I(X_1; Y|X_2), C_1 + C_2 - I(X_1; X_2), I(X_1, X_2; Y) - I(X_1, X_2; Z)) \tag{33}$$

is obtained. From the standard discretization procedure [11], $R_{\mathrm{DF}}^{(1)}(\rho)$ and $R_{\mathrm{PDF-M}}^{(1)}(\rho)$ are obtained by evaluating (23) and (33) for the degraded Gaussian diamond-wiretap channel discussed in Section II and a jointly Gaussian distribution $p(x_1, x_2)$ such that x_k for $k \in [1:2]$ has zero mean and variance of P_k and the correlation coefficient between X_1 and X_2 is $\rho \in [-1, 1]$.

C. Proof of Theorem 4

We note that the upper bound (9) continues to hold when the fictitious message is given only at the source. Then, we have

$$\begin{aligned} nR &\le I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n \qquad (34)\\ &\le I(X_1^n, X_2^n; J_1, Y^n) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n\\ &\le H(J_1) + I(X_1^n, X_2^n; Y^n|J_1) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n\\ &\overset{(a)}{\le} H(J_1) + I(X_2^n; Y^n|J_1, X_1^n) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n\\ &\le nC_1 + I(X_2^n; Y^n|X_1^n) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n\\ &\overset{(b)}{\le} nC_1 + n\log(1 + (1-\lambda_b^2)P_2) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n \qquad (35)\end{aligned}$$

where λ_b is defined in the proof of Theorem 1, (a) is because X_1^n is a function of J_1, and (b) is from some similar steps as in the derivation of (3). Similarly, we can obtain

$$nR \le nC_2 + n\log(1 + (1-\lambda_a^2)P_1) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n, \qquad (36)$$

where λ_a is defined in the proof of Theorem 1.

For any random variable U_i generated through a conditional pmf $p(u_i|x_{1,i}, x_{2,i}, y_i)$, we have

$$\begin{aligned} nR &\le I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n\\ &\le H(X_1^n, X_2^n) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n\\ &\le H(X_1^n) + H(X_2^n) - I(X_1^n; X_2^n) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n\\ &\overset{(a)}{\le} nC_1 + nC_2 - I(X_1^n; X_2^n) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n \qquad (37)\\ &\overset{(b)}{\le} nC_1 + nC_2 - I(X_1^n, X_2^n; U^n) + I(X_1^n; U^n|X_2^n)\\ &\qquad + I(X_2^n; U^n|X_1^n) - I(X_1^n, X_2^n; Z^n) + n\epsilon_n, \qquad (38)\end{aligned}$$

where (a) is because X_k^n is a function of J_k for $k \in [1:2]$ and (b) is from some similar steps as in the derivation of (7).

Note that we have the following lower and upper bounds on $\frac{1}{n}h(Y^n)$:

$$\begin{aligned}\frac{1}{n}h(Y^n) &\ge \frac{1}{n}h(Y^n|X_1^n, X_2^n) = \frac{1}{n}h(N_Y^n) = \frac{1}{2}\log(2\pi e)\\ \frac{1}{n}h(Y^n) &\le \frac{1}{2}\log(2\pi e)(1 + P_1 + P_2 + 2\sqrt{P_1P_2}).\end{aligned}$$

Hence, there exists $\rho \in [-\bar{\rho}, 1]$ such that

$$\frac{1}{n}h(Y^n) = \frac{1}{2}\log(2\pi e)(1 + P_1 + P_2 + 2\rho\sqrt{P_1 P_2}). \tag{39}$$

Then, we have the following lower bound on $I(X_1^n, X_2^n; Z^n)$:

$$I(X_1^n, X_2^n; Z^n) \geq \frac{n}{2}\log(1 + g(P_1 + P_2 + 2\rho\sqrt{P_1 P_2})) \tag{40}$$

from the entropy power inequality.

Now, we are ready to prove Theorem 4. First consider $\rho \in [-\bar{\rho}, 0)$. Then, from (34)-(37), (39), and (40), we have $R \leq \min(f_1(0), f_2(0), f_3(0), f_4(\rho)) - f_5(\rho) + \epsilon_n$. Next, consider $\rho \in [0, 1]$. Then, due to similar reasons as in the proof of Theorem 1, we have $\rho \leq \min(\lambda_a, \lambda_b)$. Then, from (34)-(37), (39), and (40), we have $R \leq \min(f_1(\rho), f_2(\rho), f_3(0), f_4(\rho)) - f_5(\rho) + \epsilon_n$. Now, assume that ρ further satisfies $\rho \in [0, \rho^*]$. We choose $U_i = Y_i + \tilde{V}_i$, where $\tilde{V}_i$ is an i.i.d. Guassian random variable with zero mean and variance of $\tilde{\gamma} = \sqrt{P_1 P_2}(\frac{1}{\rho} - \rho) - 1$. Then, by substituting (40) and similar bounds as (17)-(19) to (38), we obtain $R \leq f_3(\rho) - f_5(\rho) + \epsilon_n$. Hence, we have $R \leq \min(f_1(\rho), f_2(\rho), f_3(\rho), f_4(\rho)) - f_5(\rho) + \epsilon_n$ for $\rho \in [0, \rho^*]$. This concludes the proof of Theorem 4.

D. Proof of Theorem 5

As in the proof of Theorem 2, we first assume that the channel from the relays to the legitimate destination and the eavesdropper is a discrete memoryless channel with a conditional pmf $p(y, z|x_1, x_2)$. Fix $p(x_1, x_2)$ and $\epsilon > 0$. Let

$$R' = I(X_1, X_2; Z) - \delta(\epsilon). \tag{41}$$

For the DF scheme, by letting the source send both the message and the fictitious message to the relays, an achievable secrecy rate of

$$\min(C_1 - R', C_2 - R', I(X_1, X_2; Y) - I(X_1, X_2; Z)) \tag{42}$$

is obtained from (23) by replacing C_1 and C_2 by $C_1 - R'$ and $C_2 - R'$, respectively.

Similarly, for the PDF-DF-M scheme, by letting the source send the fictitious message as well as the partial message and the relay codeword index to relay k for $k = 1, 2$ in the PDF-M scheme for the first scenario, an achievable secrecy rate of

$$\begin{aligned}\min(&C_1 + I(X_2; Y|X_1) - R',\ C_2 + I(X_1; Y|X_2) - R',\\ &C_1 + C_2 - I(X_1; X_2) - 2R', I(X_1, X_2; Y) - I(X_1, X_2; Z))\end{aligned} \tag{43}$$

is obtained from (33) by replacing C_1 and C_2 by $C_1 - R'$ and $C_2 - R'$, respectively.

The PDF-PDF-M scheme is described in the following.

- Codebook generation: We represent the message $w \in [1 : 2^{nR}]$ and the fictitious message $m \in [1 : 2^{nR'}]$ as a partial message pair $(w_1, w_2) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$ and a partial fictitious message pair $(m_1, m_2) \in [1 : 2^{nR'_1}] \times [1 : 2^{nR'_2}]$, respectively, for some nonnegative rates R_1, R_2, R'_1, and R'_2 such that

$$R_1 + R_2 = R,\ R'_1 + R'_2 = R'. \tag{44}$$

  Consider $\tilde{R}_k \geq 0$ for $k \in [1 : 2]$. For each $k \in [1 : 2]$ and $(w_k, m_k, l_k) \in [1 : 2^{nR_k}] \times [1 : 2^{nR'_k}] \times [1 : 2^{n\tilde{R}_k}]$, generate $x_k^n(w_k, m_k, l_k)$ independently according to $\prod_{i=1}^n p(x_{k,i})$.
- Encoding at the source: For message (w_1, w_2) and fictitious message (m_1, m_2), the source finds an (l_1, l_2) such that

$$(x_1^n(w_1, m_1, l_1), x_2^n(w_2, m_2, l_2)) \in \mathcal{T}_\epsilon^{(n)}.$$

  For $k \in [1 : 2]$, the source sends (w_k, m_k, l_k) to relay k.
- Encoding at relay $k \in [1 : 2]$: After receiving (w_k, m_k, l_k) from the source, relay k sends $x_k^n(w_k, m_k, l_k)$.
- Decoding at the legitimate destination: The legitimate destination finds $(\hat{w}_1, \hat{w}_2, \hat{m}_1, \hat{m}_2, \hat{l}_1, \hat{l}_2)$ such that

$$(x_1^n(\hat{w}_1, \hat{m}_1, \hat{l}_1), x_2^n(\hat{w}_2, \hat{m}_2, \hat{l}_2), y^n) \in \mathcal{T}_\epsilon^{(n)}.$$

  The legitimate destination declares $(\hat{w}_1, \hat{w}_2)$ is the message.
- Error analysis: From the mutual covering lemma, the encoding error at the source averaged over the codebooks tends to zero as n tends to infinity if

$$\tilde{R}_1 + \tilde{R}_2 > I(X_1; X_2) + \delta(\epsilon). \tag{45}$$

  For $k \in [1 : 2]$, the transmission of (w_k, m_k, l_k) from the source to relay k requires

$$R_k + R'_k + \tilde{R}_k < C_k. \tag{46}$$

  From the standard error analysis, the decoding error at the legitimate destination averaged over the codebooks tends to zero as n tends to infinity if

$$R_1 + R'_1 + \tilde{R}_1 < I(X_1; Y|X_2) + I(X_1; X_2) - \delta(\epsilon) \tag{47}$$

$$R_2 + R'_2 + \tilde{R}_2 < I(X_2; Y|X_1) + I(X_1; X_2) - \delta(\epsilon) \tag{48}$$

$$R_1 + R_2 + R'_1 + R'_2 + \tilde{R}_1 + \tilde{R}_2 < I(X_1, X_2; Y) + I(X_1; X_2) - \delta(\epsilon). \tag{49}$$

- Secrecy analysis: We can show $\lim_{n\to\infty}\frac{1}{n}I(W;Z^n|\mathcal{C})\leq\delta(\epsilon)+\epsilon$ if (41) and the following inequalities are satisfied.

$$R_1'+\tilde{R}_1<I(X_1;Z|X_2)+I(X_1;X_2)-\delta(\epsilon) \tag{50}$$

$$R_2'+\tilde{R}_2<I(X_2;Z|X_1)+I(X_1;X_2)-\delta(\epsilon) \tag{51}$$

$$R_1'+R_2'+\tilde{R}_1+\tilde{R}_2<I(X_1,X_2;Z)+I(X_1;X_2)-\delta(\epsilon) \tag{52}$$

  See Section IV-E for the detail.

Therefore, there exists a sequence of codes such that $P_e^{(n)}$ tends to zero and $\frac{1}{n}I(W;Z^n)\leq\delta(\epsilon)+\epsilon$ as n tends to infinity if (41), (44)-(52) are satisfied. By performing Fourier-Mozkin elimination to (41), (44)-(52) and by taking $\epsilon\to 0$, a secrecy rate of

$$\min(C_1+I(X_2;Y|X_1),C_2+I(X_1;Y|X_2),C_1+C_2-I(X_1;X_2),I(X_1,X_2;Y))-I(X_1,X_2;Z) \tag{53}$$

subject to the constraints

$$C_1>I(X_1;Z),C_2>I(X_2;Z) \tag{54}$$

is obtained. From the standard discretization procedure, $R_{\text{DF}}^{(2)}(\rho)$, $R_{\text{PDF}-\text{DF}-\text{M}}^{(2)}(\rho)$, and $R_{\text{PDF}-\text{PDF}-\text{M}}^{(2)}(\rho)$ are obtained by evaluating (42), (43), (53), and (54) for the degraded Gaussian diamond-wiretap channel discussed in Section II and a jointly Gaussian distribution $p(x_1,x_2)$ such that x_k for $k\in[1:2]$ has zero mean and variance of P_k and the correlation coefficient between X_1 and X_2 is $\rho\in[-1,1]$.

E. Secrecy analysis

Let $\mathcal{C}$ denote the random codebook. For message W, fictitious message M, and chosen relay codeword indices $L=(L_1,L_2)$, we have

$$\begin{aligned}
H(W|Z^n,\mathcal{C}) &= H(W,M,L|Z^n,\mathcal{C})-H(M,L|W,Z^n,\mathcal{C})\\
&\overset{(a)}{\geq} H(W,M,L|Z^n,\mathcal{C})-n\epsilon\\
&= H(W,M,L|\mathcal{C})-I(W,M,L;Z^n|\mathcal{C})-n\epsilon\\
&\geq H(W)+nR'-I(W,M,L,X_1^n,X_2^n,\mathcal{C};Z^n)-n\epsilon\\
&= H(W)+nR'-I(X_1^n,X_2^n;Z^n)-n\epsilon\\
&\geq H(W)+nR'-nI(X_1,X_2;Z)-n\epsilon\\
&= H(W)-n\delta(\epsilon)-n\epsilon
\end{aligned}$$

for sufficiently lage n, where (a) is because the eavesdropper who already knows W and Z^n can decode M and L with high probability when (30)-(32) are satisfied for the first scenario and when (50)-(52) are satisfied for the second scenario. Hence, we have $\lim_{n\to\infty} \frac{1}{n} I(W; Z^n|\mathcal{C}) \leq \delta(\epsilon) + \epsilon$.

V. Conclusion

In this paper, we derived nontrivial upper and lower bounds on the secrecy capacity of the degraded Gaussian diamond-wiretap channel under two scenarios regarding the availability of randomness.

Our upper bound was obtained by taking into account the correlation between the two relay signals and the availability of randomness at each encoder, which generalizes both the upper bound on the capacity of the diamond channel without secrecy constraint [3] and the upper bound on the sum secrecy capacity of the MAC wiretap channel [4]. For the lower bound, we proposed DF scheme and partial DF scheme incorporated with multicoding that is called PDF-M scheme for the first scenario and PDF-DF-M and PDF-PDF-M schemes for the second scenario depending on whether the relay decodes the whole or partial fictitious message. In the first scenario, PDF-M scheme with strictly positive correlation coefficient was shown to outperform DF and PDF (without multicoding) schemes for some channel parameters. We also showed that the PDF scheme is asymptotically optimal for the first scenario when at least one of relay power constraint tends to infinity. For the second scenario, we presented a condition for channel parameters where the PDF-PDF-M scheme is optimal. Furthermore, because the fictitious message has to be sent through the BC for the second scenario, it was shown to be befinicial to consider negative correlation in all DF, PDF-DF-M, PDF-PDF-M schemes when the BC cut becomes the bottleneck. Furthermore, we investigated the effect of the presence of an eavesdropper on the capacity. If there is a sufficient amount of common randomness between the source and the relays, it was shown that there is no decrease in capacity due to an eavesdropper for some range of C.

As a final remark, it seems to be straightforward to combine our DF scheme and partial DF scheme incorporated with multicoding by using superposition coding, but the resultant rate expression would be rather complicated with less useful insights.

References

[1] B. E. Schein, "Distributed coordination in network information theory," Ph.D. dissertation, Massachusetts Institute of Technology, 2001.

[2] D. Traskov and G. Kramer, "Reliable communication in networks with multi-access interference," in *Proc. IEEE Information Theory Workshop (ITW)*, 2007, pp. 343–348.

[3] W. Kang and N. Liu, “The Gaussian multiple access diamond channel,” in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Jul.-Aug. 2011, pp. 1499–1503.

[4] E. Tekin and A. Yener, “The Gaussian multiple access wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 54, pp. 5747–5755, Dec. 2008.

[5] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *Proc. Advances in Cryptology (CRYPTO ’99)*, 1999, pp. 388–397.

[6] D. Kobayashi, H. Yamamoto, and T. Ogawa, “How to attain the ordinary channel capacity securely in wiretap channels,” in *Proc. IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, Oct. 2005, pp. 13–18.

[7] R. A. Chou and M. R. Bloch, “Uniform distributed source coding for the multiple access wiretap channel,” in *Proc. IEEE Conference on Communications and Network Security (CNS)*, Oct. 2014, pp. 127–132.

[8] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[9] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[10] A. El Gamal and E. C. van der Meulen, “A proof of Marton’s coding theorem for the discrete memoryless broadcast channel,” *IEEE Trans. Inf. Theory*, vol. 27, pp. 120–122, Jan. 1981.

[11] R. J. McEliece, *The theory of information and coding*. Addison-Wesley, Reading, 1977.